ISSUES IN DEFENCE SCIENCE & TECHNOLOGY

ISSUE 3, FEBRUARY 1998

Issues in Defence Science & Technology is published on an ad hoc basis by the Defence Research & Development (R&D) Branch. Its aim is to provide senior officers and managers within the Department of National Defence with expert scientific and technical knowledge, which enhances their ability to make informed decisions.

For more information on the Defence R&D Branch's *Modern Communications Electronic Warfare* initiatives, please contact Andrew Mudry, Electronic Support Measures, DREO, ph: (613) 998-2118, e-mail: Andrew.Mudry@dreo.dnd.ca, or Dr. Malcolm Vant, Deputy Scientific Advisor (Command & Control Information Systems), ph: (613) 992-6601, e-mail: Malcolm.Vant@crad.dnd.ca.

Modern Communications Electronic Warfare

THE ISSUE IN CONTEXT

The communications Electronic Warfare (EW) capabilities of the Canadian Forces (CF) are in the process of being reshaped to respond to the significant threat posed by the emerging tactical deployment of modern mobile communications systems, and the increased integration of military and civilian telecommunications systems.

The diverse array of electromagnetic target signals presented during modern conflict poses new and unique challenges to EW equipment and tactics.

BACKGROUND

Communications EW tactics are non-lethal force multipliers that have proven effective at all levels of conflict. These tactics may be classed as either Electronic Support Measures (ESM) or Electronic Counter Measures (ECM).

ESM techniques are dedicated to the interception of an adversary's communications for the purpose of tactical Signals Intelligence (SIGINT) production, which provides an indication of an adversary's intentions. The location of adversary transmitters, using radio direction-finding techniques, is also an important part of ESM.

ECM techniques involve the disruption of adversary command and control functions via radio-jamming operations, or via the insertion of false instructions into the adversary command and control hierarchy.

Throughout the Cold War, communications EW research and development focused largely on the threat posed by Combat Net Radio (CNR) systems in a high-intensity European conflict. State-of-the-art wireless communications were led by the military as it strived to incorporate Low Probability of Interception (LPI) and other security features on these CNR systems.

Developments occurred at a relatively slow pace, as deployed equipment tended to remain in service for many years. Since the end of the Cold War, however, three key trends have been observed:

1. The civilian rather than the military sectors now set state of the art in wireless communications. Several global systems capable of providing wireless point-to-point communications virtually anywhere in the world already exist, and the future integration of terrestrial cellular systems and satellite-based personal communications systems will further ensure global coverage.

2. Military users, knowing the reliability and convenient features available on civilian networks, are demanding no less from their tactical communications systems. Military communicators may set up dedicated military networks using civilian equipment, or simply buy capacity on civilian networks, thereby integrating the military and civilian communications infrastructures.

   Various military and paramilitary forces around the world have exercised both options and wireless access to the Public Switched Telephone Network (PSTN) is evolving into the communications resource of choice for many military users in low- to medium-intensity conflict situations.

3. The threat of a high-intensity global conflict has diminished significantly and the CF are more likely to become involved in peacekeeping operations or low-intensity conflict associated with regional disputes around the world.

   Commercial mobile communications systems and the PSTN will remain intact in such situations, and act as resources available to both sides in the conflict.

The potential use of civilian equipment or networks by foreign military forces represents a drastic change in the target array presented to CF EW operators and poses several unique problems for both ESM and ECM operations.

In the case of ESM, intercept operators are now presented with a large number of signals, only a few of which come from military users of interest. In addition, ESM operators must deal with a wide and rapidly changing array of communications standards and protocols, and must also sort high-priority military traffic from the civilian traffic. The growing use of encryption by non-military users complicates this sorting.

In the case of ECM, jamming operations are now complicated by the potential for interference with legitimate or even essential civilian use of the spectrum. There is also the potential for collateral damage to the communications of friendly forces that happen to be using the same commercial system. The CF must meet these challenges head-on.

R&D BRANCH ROLE

The Defence R&D Branch is firmly committed to assisting DND in preparation of effective EW capability in the modern telecommunications era, and in the transition of this EW expertise into an effective Information Operations[1] (IO) capability for the future.

This important area is one of growing investment within the R&D Branch, at a time of overall declining resources.

In order to focus and maximize the return on this investment, the Mobile Communications EW Group has been established at Defence Research Establishment Ottawa (DREO). This group is dedicated to modern communications EW threat assessment and the development of effective tactical ESM and ECM capabilities for the CF.

Where possible, existing technology is leveraged from other government departments or allied countries and adapted to meet the unique requirements of Canadian tactical EW operations. Where appropriate, the required technology is developed in-house or in cooperation with Canadian industry.

CONCLUSION

The capability of traditional EW techniques and systems is limited when pitted against modern telecommunications systems. For example, the rapid development and adoption of new communications technology has created deficiencies in the ability of U.S. forces to exploit and selectively disrupt modern signals.[2]

Cellular and personal communications systems used by civilians and hostile forces, as well as high-capacity digital, multichannel networks associated with distributed information systems, pose particularly difficult technical challenges.[3]

Likewise, the CF's ability to conduct ESM against some communications standards is limited. Such a capability is, however, essential; and since Canadian operations could conceivably take place anywhere in the world, there is a requirement that this ESM capability be easily deployable.

In the area of ECM, most currently available equipment has been designed for the barrage jamming of dedicated military communications networks. A surgical ECM capability is necessary in any modern scenario involving an integrated civilian/military telecommunications infrastructure.

This type of ECM system would allow the denial of communications to a small number of hostile military users without causing interference to legitimate civilian use of the same network.

DREO activity in mobile communications EW addresses these issues and responds to a new CF requirement driven by the ongoing integration of military and civilian communications systems.

---

1 Information Operations, also sometimes referred to as Information Warfare, is a rapidly evolving concept, which stresses achieving an information advantage against an opponent across a full range of military operations. The CF currently defines IO as "...actions taken to affect adversary information and information systems while defending one's own information and information systems" (J6 IO)
2 United States Department of Defense, Joint Warfighting Science and Technology Plan, Chapter IV, Item 4. January 1997.
3 Ibid.

(Return to Publications)

R&D Home | Search | Help | Français | Comments | D-NET Home

QUESTIONS DE SCIENCES ET TECHNOLOGIE APPLIQUÉES À LA DÉFENSE

NUMÉRO 3, FÉVRIER 1998

Questions de sciences et technologie appliquées à la Défense est une publication ponctuelle de la Direction recherche et développement pour la Défense. Elle vise à fournir des connaissances scientifiques et techniques spécialisées aux dirigeants et aux cadres du ministère de la Défense nationale afin qu'ils soient mieux en mesure de prendre des décisions éclairées.

Pour obtenir de plus amples renseignements sur les initiatives de la Direction recherche et développement pour la Défense portant sur la *guerre électronique et les réseaux modernes de télécommunications*, veuillez communiquer avec M. Andrew Mudry, Mesures de soutien électronique, CRDO, tél. : (613) 998-2118, adresse électronique : Andrew.Mudry@dreo.dnd.ca, ou M. Malcolm Vant,

Guerre électronique et réseaux modernes de télécommunications

LE CONTEXTE

Les capacités dont disposent les Forces canadiennes (FC) dans le domaine de la guerre électronique en communications sont actuellement soumises à une refonte dans le but de les adapter à l'importante menace que constituent le nouveau déploiement tactique de systèmes modernes de communications mobiles et l'intégration croissante des réseaux de télécommunications militaires et civils.

La série diversifiée de signaux de cibles électromagnétiques auxquels il faut faire face dans un conflit moderne pose des défis nouveaux et particuliers en ce qui a trait à l'équipement et aux tactiques de guerre électronique.

SITUATION

Les tactiques de la guerre électronique en communications constituent en fait une forme de recours à des multiplicateurs de force non mortelle qui ont prouvé leur efficacité à tous les niveaux de conflit. Ces tactiques peuvent être classées soit parmi les mesures de soutien électroniques (MSE), soit parmi les contre-mesures électroniques (CME).

Les MSE sont des techniques servant à intercepter les communications d'un adversaire dans le but de capter, à des fins tactiques, des renseignements sur ses transmissions (SIGINT), ce qui donne une indication des intentions de cet adversaire. La localisation des émetteurs de l'adversaire, au moyen de la radiogoniométrie, constitue également une part importante des MSE.

Les techniques utilisées comme CME visent la dislocation des fonctions de commandement et de contrôle de l'adversaire au moyen du brouillage des ondes radioélectriques ou de l'insertion de fausses instructions dans son système hiérarchique de commandement et de contrôle.

Pendant toute la période de la guerre froide, la recherche et le développement dans le domaine de la guerre électronique en communications ont porté dans une grande mesure sur la menace qu'auraient constituée les réseaux radio de combat (RRC) dans un conflit européen de haute intensité. Cherchant à intégrer des fonctions de faible probabilité d'interception et d'autres dispositifs de sécurité à ces RRC, les militaires étaient à l'avant-garde dans le domaine des télécommunications

conseiller scientifique adjoint (Systèmes d'information du commandement),
tél. : (613) 992-6601,
adresse électronique : Malcolm.Vant@crad.dnd.ca.

militaires étaient à l'avant-garde dans le domaine des télécommunications sans fil.

Le matériel déployé demeurant généralement en service pendant de nombreuses années, le rythme des développements technologiques était relativement lent. Depuis la fin de la guerre froide cependant, on a pu observer trois grandes tendances :

1. C'est à présent le secteur civil plutôt que le secteur militaire qui est à l'avant-garde technologique en matière de télécommunications sans fil. Il existe déjà plusieurs réseaux mondiaux capables d'assurer une communication sans fil de point à point pratiquement n'importe où dans le monde, et l'intégration future de systèmes cellulaires terrestres et de systèmes satellitaires de communications personnelles va accroître les capacités de couverture mondiale.

2. Les utilisateurs militaires, connaissant la fiabilité et les caractéristiques pratiques des réseaux civils, n'en demandent pas moins de leurs systèmes de télécommunications tactiques. Les spécialistes militaires des communications peuvent installer des réseaux réservés aux militaires à l'aide d'un matériel civil, ou simplement acheter de la capacité de traitement sur les réseaux civils, ce qui a pour effet d'intégrer les infrastructures militaires et civiles de télécommunications.

   Diverses forces militaires et paramilitaires à l'échelle mondiale ont opté pour un recours à ces deux possibilités et l'accès sans fil au réseau téléphonique public commuté (RTPC) est en voie de devenir, pour plusieurs utilisateurs militaires, le moyen privilégié de communication dans les conflits de faible à moyenne intensité.

3. La menace d'un conflit mondial de haute intensité a diminué de façon importante et il est probable qu'à l'avenir les FC participeront plutôt, un peu partout dans le monde, à des opérations de maintien de la paix ou à des conflits de faible intensité découlant de différends régionaux.

   Dans de telles situations, les systèmes de communications mobiles commerciaux et le RTPC demeureront intacts et constituent une ressource à la disposition des deux parties en conflit.

L'utilisation éventuelle d'équipements ou de réseaux civils par des forces militaires étrangères constitue un changement draconien dans le système d'objectifs présenté aux opérateurs - Guerre électronique (OP G ÉLEC), et soulève plusieurs problèmes très particuliers pour l'emploi de MSE ou de CME.

Dans le cas des MSE, les opérateurs d'interception captent à présent un grand nombre de signaux, dont quelques-uns seulement proviennent d'utilisateurs militaires présentant un intérêt. De plus, les opérateurs de MSE ont affaire à un large éventail de normes et de protocoles de communication qui changent constamment et ils doivent également séparer le trafic des télécommunications militaires à niveau de priorité élevé du trafic civil. Le recours croissant au chiffrement de la part des utilisateurs non militaires vient compliquer ce tri.

Dans le cas des CME, les opérations de brouillage se compliquent du fait qu'elles risquent de perturber l'utilisation légitime ou même essentielle du spectre à des fins civiles. Il existe également un risque de dommages collatéraux aux télécommunications des forces amies qui, par hasard, utiliseraient le même système commercial. Les FC doivent s'attaquer de front à ces problèmes.

RÔLE DE LA DIRECTION R ET D

La Direction R et D de la défense est fermement décidé à aider le MDN à acquérir la maîtrise technologique qu'exige la guerre électronique en cette ère des réseaux modernes de télécommunications et à traduire cette expertise en une véritable capacité de mener, dans l'avenir, des opérations liées à l'information.[1]

Cet important domaine est l'un de ceux où la Direction R et D investit d'avantage alors que les ressources diminuent de façon gobale.

Afin de concentrer les efforts et de tirer le maximum de cet investissement, on a formé, au Centre de recherche pour la défense Ottawa (CRDO), le Groupe de communications mobiles et de guerre électronique. Ce groupe se consacre à l'évaluation de la menace d'une guerre électronique moderne en communications et au développement de véritables capacités tactiques en MSE et en CME pour les FC.

Quand c'est possible, la Direction mise sur la technologie existante dont disposent d'autres ministères ou des pays alliés et l'adapte de façon à ce qu'elle réponde aux besoins particuliers des opérations canadiennes de guerre électronique tactique. Lorsqu'il y a lieu, le technologie requise est mise au point au sein de la Direction ou en coopération avec l'industrie canadienne.

CONCLUSION

La capacité des techniques et des systèmes classiques de guerre électronique est limitée lorsque l'adversaire dispose de réseaux de télécommunications modernes. À titre d'exemple, le développement rapide et l'adoption de nouvelles technologies de communication a engendré des lacunes dans la capacité des forces armées américaines d'exploiter et d'interrompre de façon sélective des signaux transmis à l'aide d'une technologie moderne.[ii]

Des problèmes techniques particulièrement difficiles se posent en ce qui a trait aux réseaux cellulaires et de communications personnelles utilisés par les civils et les forces ennemies, ainsi qu'en ce qui a trait aux réseaux multivoie numériques de grande capacité reliés à des systèmes d'information répartis.[iii]

De même, pour certaines normes de communication, la capacité des FC de recourir à des MSE est limitée. Cette capacité est pourtant essentielle et, puisque des opérations canadiennes pourraient en fait se dérouler n'importe où dans le monde, il est nécessaire qu'elle puisse être aisément déployée.

Dans le domaine des CME, la plus grande partie du matériel disponible a été conçue pour le brouillage en barrage de réseaux de communication à usage militaire exclusif. Dans tout scénario moderne de conflit dans lequel on retrouve une infrastructure intégrée de télécommunications, à la fois civile et militaire, il est nécessaire de disposer d'une capacité de recourir à des CME avec une précision chirurgicale. Avec un tel système de CME, il serait possible de bloquer les communications à un nombre limité d'utilisateurs militaires ennemis sans perturber l'utilisation civile légitime du même réseau.

Le travail du CRDO sur les communications mobiles et la guerre électronique porte sur ces aspects et répond à un nouveau besoin des FC qui découle de l'intégration progressive des réseaux de télécommunications militaires et civils.

---

i Le concept d'opérations liées à l'information - on parle parfois de guerre de l'information - évolue rapidement. Il met de l'avant la réalisation d'un avantage informationnel sur un opposant pour une gamme complète d'opérations militaires. Les FC définissent actuellement les opérations liées à l'information comme « ...des mesures prises pour perturber l'information et les systèmes d'information de l'adversaire tout en protégeant sa propre information et ses propres systèmes d'information » (J6 IO)
ii United States Department of Defense, Joint Warfighting Science and Technology Plan, chapitre IV, point 4, janvier 1997.
iii Ibidem.

(Retour à Publications)

Menu R et D | Recherche | Aide | English | Commentaires | Menu D-NET